VOLUME 19 ISSUE 2

KCJIS NEWS

MAY 2017

SHOULD YOU USE A PASSWORD MANAGER?

TAMMIE HENDRIX, TECHNICAL SECURITY AUDITOR KHP

Studies show that the average person uses a minimum of ten online passwords a day, and to remember all of these is nearly impossible. Hopefully everyone knows by now, passwords are important and you definitely don't want them falling into the wrong hands.

INSIDE THIS ISSUE

We have all tried writing them down on paper, memorizing them, using the same password for everything, and keeping all passwords in a file on your computer or phone.

Perhaps you are considering use of password management software (password manager), but is it safe? Do the benefits of using password manager software outweigh the risks?

Password managers allow you to:

- Generate and use secure, complex, and appropriately long passwords
- Never need to remember passwords – the password manager remembers them for you
- Use different passwords on different sites

A **master password** acts as the encryption key to lock away all of the others. Because a password manager is only as secure as this master password, it needs to be a good one – be sure to follow all the best practice for a robust password [1], and you need to be able to remember it! It should never be known by anyone but **you**.

As we have become accustomed, policy does not restrict nor openly approve of things like password managers.

Policy 5.6.2.1 does identify passwords as one form of **Standard Authenticator** that is *"…(the something you know, something you are, or something you have) part of the identification and authentication process.*

And, policy 5.6.3.2 goes on to say:*"…Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators."*

If you decide to use password managers, consider that:

- The biggest risk is that all of your passwords are in one place
- You can't trust just any piece of software, and
- Make sure you know how the app is saving your passwords and what risks you are taking by using it.
- The data should be encrypted with 256-bit AES [2] and have a policy of not receiving private data that is locked down with your master password.
- One threat to any software – including ones that store passwords locally - is malware. Password manager applications store passwords in a specific format at a specific location in your file system. Malware can be designed to target those locations and send anything it finds to a hacker.
    - You can help avoid malware attacks by following basic security principals like frequently updating all software, avoiding malicious websites and downloads, and avoid falling for phishing scams.
- And ALWAYS REMEMBER, there is no such thing as absolute security!

SHOULD YOU USE A PASSWORD MANAGER, CONTINUED
TAMMIE HENDRIX, TECHNICAL SECURITY AUDITOR KHP

[1] *5.6.2.1.1 Password*

Agencies shall follow the secure password attributes below, to authenticate an individual's unique ID Passwords shall:

1. *Be* ***a minimum length of eight (8) characters**** *on all systems*
2. *Not be a dictionary word or proper name*
3. *Not be the same as the User ID*
4. *Expire within a maximum of 90 calendar days*
5. *Not be identical to the previous ten (10) passwords*
6. *Not be transmitted in the clear outside the secure location*
7. *Not be displayed when entered*

* The longer the password the better! Passwords should also include at least three of the four character sets: Upper case letters, lower case letters, numbers (0-9), and special characters like ?@#$ %^&*().

[2] Refer to KCJIS Policy and Procedures 5.10.1.2 for encryption policies, where in part it states:

3. *When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).*
    - *a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:*
        - *i. Be at least 10 characters*
        - *ii. Not be a dictionary word*
        - *iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character*
        - *iv. Be changed when previously authorized personnel no longer require access*
    - *b) Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.*

KIBRS REPORTING DEADLINES FOR 2017 REPORTS
MITCH BEEMER, INCIDENT BASED REPORTING UNIT MANAGER KBI

The Incident Based Reporting Section (IBR) at the Kansas Bureau of Investigation would like to remind all local law enforcement agencies of all upcoming deadlines in 2017. The IBR Section does not guarantee inclusion in state and federal publications if your agency does not submit the required reports by the deadline.

April 17, 2017: First Quarter deadline. Submit January - March 2017 reports to the KBI headquarters.
July 17, 2017: Mid-Year deadline. Submit January - June 2017 reports to the KBI headquarters. Data submitted by this deadline will be included in semi-annual statistic reports, such as the FBI's *Semiannual UCR Report*.
October 16, 2017: Third Quarter deadline. Submit January - September 2017 reports to the KBI headquarters.
January 15, 2018: Fourth Quarter deadline. Submit January - December 2017 reports to the KBI headquarters.
February 22, 2018: Final deadline for submission of all 2017 reports to the KBI. Data submitted by this deadline will be included in the FBI Crime in the United States publication and other annual statistic reports.

The Law Enforcement Officers Killed and Assault (LEOKA) reports, Supplemental Homicide Reports, and the Zero Reports are due by the 15th of the following month. For example, if an agency is sending data for the month of November they should submit the November reports by December 15th. If the 15th falls on a weekend or holiday, the deadline is extended to the next business day.

NEWS FROM THE KBI HELP DESK

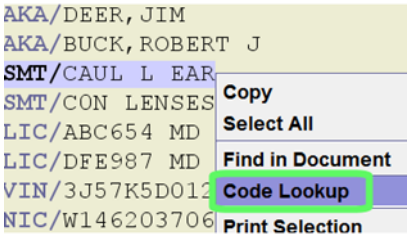
JAVIER BARAJAS, NETWORK CONTROL TECHNICIAN III KBI
JEFFREY DOWNING, NETWORK CONTROL TECHNICIAN III KBI
LAURA BOHNENKEMPER, IT PROJECT MANAGER KBI

Did You Know?

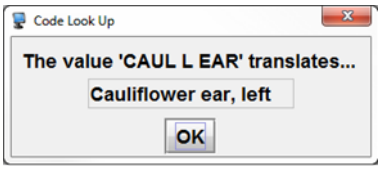
Did you know you can lookup codes in a response? Have you ever received a response message that contained an National Crime Information Center (NCIC) code and didn't know what the code meant? Instead of having to go to the NCIC Code Manual, you can have Messenger translate the code for you. First, you will need to highlight the Message Field Code (MFC) and the code value in the response text. The MFC is (typically) the three-letter abbreviation for the field name. You need to highlight that portion, the slash character, and the code value. For example, SMT/ CAUL L EAR for the NCIC scars, marks and tattoos code.

```
AKA/DEER,JIM
AKA/BUCK,ROBERT J
SMT/CAUL L EAR
SMT/CON LENSES
```

Once the MFC and code are highlighted, right-click on the message display and choose the 'Code Lookup' item from the popup menu.



Messenger will look up the code value and display it in the popup box.



Alternatively, you can look up the code value by highlighting the relevant portion of the response and press the F1 key. Note: you can select vehicle make, model, and style codes at the same time.

Save the Date!

The annual KCJIS Conference is scheduled for June 4-6, 2017 at the Ramada Inn Hotel in Topeka, Kansas. The agenda is posted on the KCJIS web portal under the Information tab – KS State Systems – KCJIS section. Register soon on Kansas.gov!

KCJIS NE KS User Group

At the March meeting the group received an update on KS Warrant Conversion to NCIC from Kansas Bureau of Investigation (KBI) IT staff. Topeka PD presented on their validation letter process. The Mail Merge type setup was emailed to members of the NE KS User Group. The March meeting ended with a tour of the KBI Lab on Washburn University's campus. Our next meeting is on May 4th, 2017 starting at 12:00PM in the Auditorium at the KBI Headquarters building in Topeka.

Java 8 Update 71

Java 8 Update 71 is now available for download via the CPI Desktop Website

NEWS FROM THE KBI HELP DESK, CONTINUED
JAVIER BARAJAS, NETWORK CONTROL TECHNICIAN III KBI
JEFFREY DOWNING, NETWORK CONTROL TECHNICIAN III KBI
LAURA BOHNENKEMPER, IT PROJECT MANAGER KBI

Federal Grant Available

The Federal Edward Byrne Memorial Justice Assistance Grant may assist in funding Computer Aided Dispatch (CAD) server upgrades. Official purpose areas and other consideration for use of this grant can be found on the State of Kansas Grants Program website. The application deadline is set for August 2017. The grant will begin on Oct 1, 2017 and end Sept 30, 2018.

NB Registration Records Accessed via Nlets

Nebraska Legislative Bill (LB) 53 which took effect on January 1, 2017 provides the following:

Upon the owner's request, one license plate may be issued for any passenger car which is not manufactured to be equipped with a license plate bracket on the front of the vehicle.

For those owners who select this option a decal shall be issued with the license plate which shall be displayed on the driver's side of the windshield. An additional $100 non-refundable fee plus the cost of the decal (60¢) shall be collected at the time of registration on an annual basis.

For new cars, the customer is responsible for determining/indicating if a front plate bracket exists; there are no lists available of vehicle makes, etc. which qualify. Any new car may be manufactured without a bracket.

For those cars which have previously been registered in Nebraska and the owner requests a single plate; proof that a front plate bracket exists is not necessary. However, the customer should be asked if a bracket is present (or where the previous plate was displayed). If the plate was displayed on the front of the vehicle, the vehicle does not qualify for the single plate option.

The issuance of the one-plate decal is now indicated on the registration record as *SINGLE PLATE* to the right of the license plate number.

Identity and Access Management (IAM)

Here at the KBI we have been working hard to modernize the security architecture of the Kansas Criminal Justice Information System (KCJIS). Currently we are in phase two working on an application for Identity and Access Management (IAM) to replace the Kansas Consumer Information System (KACIS) and add much more functionality for the terminal agency coordinators (TACs) to manage their agency users. For example, you will be able to assign tokens without having to contact the Help Desk and request application access for users all within the application.

In addition, we are looking for feedback from agency TACs to improve on the reporting capability of the new IAM. Currently, KACIS has a group of predefined reports. As an agency TAC, what types of reports are of interest to you? Reports can include: Token information for my agency or agency that I serve, an email list of TACs for other agencies, or something else. Please take a few minutes to review the available reports in KACIS and provide suggestions and feedback to the KBI Help Desk at HelpDesk@kbi.state.ks.us

We look forward to showing you more about the new IAM at the KCJIS conference. Keep a lookout for those presentations on the KCJIS conference schedule.

44TH ANNUAL NLPOA TRAINING CONFERENCE
DARRIN FULTON,NLPOA NE KS CHAPTER PRESIDENT

The National Latino Peace Officers Association (NLPOA) will be holding its 44th Annual National Training Conference October 11-14, 2017 at the Great Wolf Lodge in Kansas City, KS. The conference includes a half day forum featuring law enforcement leaders from around the country in addition to two days of law enforcement training from local and national law enforcement trainers including Calibre Press, Code 9 Project, The Guidestone Group, National Tactical Officers Association (NTOA), Kansas Bureau of Investigation (KBI), and others. Additionally, on the evening of Friday, October 13th, Paul Rodriguez and three other comedians will host a comedy night to benefit the families Captain Melton, Detective Lancaster, and Deputy Collins. To register for the conference, go to http://nlpoanekansas.com. The price for non-members is $300 which will pay for training and lunch for two days.

TRANSACTION NUMBERS
KRISTI CARTER, CRIMINAL HISTORY RECORDS UNIT MANAGER KBI

A Transaction Number is a unique (non-reusable) number assigned to a series of events that are related to a single arrest (including notice to appear (*NTA)* issuances and *Summons*). Those related events are one record transaction termed a "cycle" within the rap sheet and are used to clearly associate the history of the actions and dispositions that occur as a result of that arrest or summons. Transaction numbers also serve to associate related events within different databases such as the Automated Fingerprint Identification System (AFIS), the Kansas Computerized Criminal History (CCH) database, and the Kansas Incident Based Reporting System (KIBRS).

A transaction number is assigned when an individual is arrested for a felony, class A or B misdemeanor, or a class C assault and is assigned at the time of fingerprint submission. A transaction number may also be assigned upon fingerprinting for an event in which the subject was issued a summons or notice to appear.

It is extremely important that the transaction number follows from the arrest to the prosecutor and on to the court as they are used to match the fingerprint card to the Kansas Disposition Report (KDR) completing a cycle on the criminal history record. This communication is equally important during electronic disposition reporting. If the transaction number at the time of the electronic submission does not match the transaction number at the time of the arrest, then the disposition does not go directly to the criminal history record. Rather, it waits in a queue to be reviewed and processed by records staff at the Kansas Bureau of Investigation (KBI) in the order it is received. A significant increase in the amount of time from submission to posting on the criminal history record will result. This may also cause the disposition to appear as unrelated to the arrest on the rap sheet.

A transaction number is used for only one event and for only one person. Numerous charges may be under one transaction number and the charges may pertain to numerous jurisdictions. If charges pertain to more than one jurisdiction, to include Municipal versus District Court, the arresting agency should ensure that a copy of the KDR with the transaction number is forwarded to all pertinent entities.

2017 KCJIS CONFERENCE
AMY JOHNSON, CJIS UNIT KHP

REGISTRATION IS NOW OPEN!

Join us for the

17TH ANNUAL KCJIS CONFERENCE

June 4 – 6, 2017

Ramada Inn & Conference Center in Topeka

CONFERENCE SCHEDULE & REGISTRATION
IS NOW AVAILABLE VIA CJIS LAUNCH PAD

This year attendees will have the option of touring the new KBI Forensic Science Center as part of the conference schedule. Availability for the tours are limited to the first 120 people who register for the tour online through the conference registration link. If you have already had the opportunity to tour the KBI Forensic Science Center, please allow others who have not toured the Forensic Science Center an opportunity to go see it.

Reserve your room today by contacting Ramada Inn at 785.234.5400 and mention you are with the KCJIS Conference. Room rates are set at $83.

MISSING PERSONS DATABASE
JENNIFER SLAGLE, MISSING PERSONS CLEARINGHOUSE MANAGER KBI

The Kansas Bureau of Investigation (KBI) is almost ready to launch the new Missing Persons Database! This new database will allow the public to access profiles, consisting of images and information, of those who have been reported as missing in Kansas in the hopes that it will increase the likelihood of finding a missing person.

When a report of a missing person is made, the information is entered into the National Crime Information Center (NCIC). Images will then be uploaded into the KBI Missing Persons Database which will be located in the Kansas Criminal Justice Information System (KCJIS) Web Portal.

We are asking agencies with open missing person's cases, which are validated in NCIC, to go to the Missing Persons Database and upload images for new and previously opened cases. Please ensure that written permission is obtained prior to uploading images on the missing person's cases. A copy of the permission form will be located in the Missing Persons Database. The permission form will need to be retained by the law enforcement agency and a copy will need to be forwarded to the KBI at Missing.Persons@kbi.state.ks.us.

How to upload images to the database:

All KCJIS users will have access to the Missing Persons Database. When a user logs into the KCJIS Web Portal, there will be a Missing Persons icon next to the KCJIS Portal icon.

There will be two ways to locate a missing person's record:

Option #1:

Search by "Active Agency Missing Persons" which will be on the home page of the Missing Persons Database. Click on "View Records" and a list of all active missing persons records for your agency ORI will appear.

Option #2:

Click on the Missing dropdown button at the top of the screen and perform a "Missing Persons Search." The specific record you are searching for will appear.

To upload an image to a missing person's record, click on the "Add Images" link. This will take you to a file upload page where you can upload a single or multiple images at one time. Click on the "Choose Files" button and then select the image(s) you want to upload. Press the "Upload" button. Supported image file types are .jpg, .jpeg, .png, .tif, and .gif.

Agencies may only upload images to missing person's records for which their agency is listed as the Originating ORI.

Now that we have the capability…let's make the information available for the public so they can help us find those who are missing and bring them home!

If you have questions about this process, please contact Jennifer Slagle by email at Jennifer.Slagle@kbi.state.ks.us or by telephone at (785) 296-8221.

AFIS ADMINISTRATIVE MESSAGES TRAINING
TINA ORTEGA, IDENT UNIT/FIELD SUPPORT TRAINER KBI

CALLING ALL DISPATCHERS

Are you attending this year's Kansas Criminal Justice Information Systems (KCJIS) Conference on June 5th and 6th? If so, please plan to attend my training session. This session will cover the Automated Fingerprint Identification System (AFIS) administrative messages received by your agency on the KCJIS terminal. Multiple messages are generated once a fingerprint submission has been received electronically or manually and processed. Each message will be discussed to give the operator a better understanding of the need/use for this information. If you are unable to attend and would like more information, please contact Tina Ortega at (785) 296-4483 or email tina.ortega@kbi.state.ks.us.

WINDOWS VISTA
DON CATHEY, KCJIS INFORMATION SECURITY OFFICER KHP

Windows Vista
January 30, 2007 – April 11, 2017

Windows Vista reached its end of life (EOL) for extended maintenance support on April 11, 2017. Here is part of the obituary as provided on Microsoft's lifecycle web page: http://windows.microsoft.com/en-us/windows/lifecycle.

"After April 11, 2017, Windows Vista customers will no longer receive new security updates, non-security hotfixes, free or paid assisted support options, or online technical content updates from Microsoft.

If you continue to use Windows Vista after support has ended, your computer will still work but ***it might become more vulnerable to security risks and viruses.*** *Internet Explorer 9 is no longer supported, so* ***if your Windows Vista PC is connected to the Internet and you use Internet Explorer 9 to surf the web, you might be exposing your PC to additional threats****. Also, as more software and hardware manufacturers continue to optimize for more recent versions of Windows, you can expect to encounter more apps and devices that do not work with Windows Vista.*

Microsoft has also stopped providing Microsoft Security Essentials for download on Windows Vista. If you already have Microsoft Security Essentials installed, you'll continue to receive antimalware signature updates for a limited time. However, please note that Microsoft Security Essentials (or any other antivirus software) will have limited effectiveness on PCs that do not have the latest security updates. This means that PCs running Windows Vista will not be secure and will still be at risk for virus and malware."

KCJIS and FBI CJIS Security Policy **5.10.4.1 Patch Management** requires consistent systems patching w*hich cannot be accomplished without maintenance support*. Therefore, as was the case with its older brother Windows XP, ***Windows Vista users will no longer be compliant***, and more importantly, their own enterprise and any connected enterprises with which they share a trust relationship becomes vulnerable to exploits associated with out of date operating systems.

UPCOMING KBI TRAINING OPPORTUNITIES
JESSICA CROWDER, PROGRAM CONSULTANT I KBI

The next training opportunity with the Kansas Bureau of Investigation (KBI) will take place at Headquarters in Topeka on June 28th and 29th. See the schedule below for classes offered. To attend this complimentary training, please register with the KBI receptionist at AnnexFrontDesk@kbi.state.ks.us or (785) 296-7404. When registering please include the following information: specific date, class, and the number of attendees from your agency. Also, please provide an email or phone number for follow-up confirmation. Register early as seating is limited!

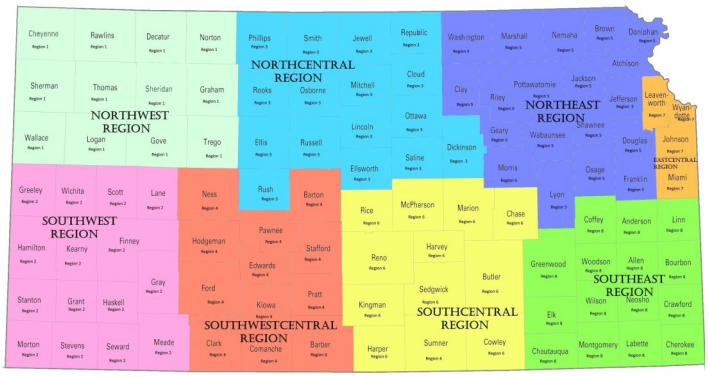
Wednesday, June 28th		
KBI Auditorium (HQ)	**KBI Training Room (Annex)**	**Time**
Offender Registration	Criminal History Records	8:30am—12:00pm
KsORT	Rapsheet Differences	1:00pm—4:30pm

Thursday, June 29th		
KBI Auditorium (HQ)	**KBI Training Room (Annex)**	**Time**
KIBRS	Missing Persons	8:30am—12:00pm
Case Inquiry	10 Print Identification	1:00pm—4:30pm

KCJIS USER GROUPS
MELISSA WEISGERBER, IT PROGRAM CONSULTANT KBI

For the past year, there has been talk about Kansas Criminal Justice Information System (KCJIS) User Groups starting in different regions. We have received some feedback from those that are interested in attending these groups. We have set regions, and each county within each region is listed below. Emails will be going out to all TACs to inform them that we are trying to get initial meetings set up. Don't panic as we may be coming to you to host the first meeting as a meet and greet to help provide you an idea of how the meetings are conducted. We are still looking for places to host meetings, as well as volunteers to conduct the meetings, take the minutes, and help put an agenda together for the meetings. We hope that as we get these groups up and running, that the duties and obligations will rotate so that it is not always the same person or group in charge so that we all can contribute to more of a team atmosphere. We would also like for the meetings to rotate in location, so that we the KBI can better serve you.

PROPOSED KCJIS USER GROUPS REGIONS



DRAFT COPY

NorthWest Region
Cheyenne
Sherman
Wallace
Rawlins
Thomas
Logan
Decatur
Sheridan
Gove
Norton
Graham
Trego

NorthCentral
Cloud
Dickinson
Ellis
Ellsworth
Jewell
Lincoln
Mitchell
Osborne
Ottawa
Phillips
Republic
Rooks
Rush
Russell
Saline
Smith

SouthCentral
Butler
Chase
Cowley
Harper
Harvey
Kingman
Marion
McPherson
Reno
Rice
Sedgwick
Sumner

SouthEast
Allen
Anderson
Bourbon
Chautauqua
Cherokee
Coffey
Crawford
Elk
Greenwood
Labette
Linn
Montgomery
Neosho
Wilson
Woodson

SouthWest Region
Greely
Hamilton
Stanton
Morton
Wichita
Kearny
Grant
Stevens
Scott
Finney
Haskell
Seward
Lane
Gray
Meade

SouthWestCentral
Barber
Barton
Clark
Comanche
Edwards
Ford
Hodgeman
Kiowa
Ness
Pawnee
Pratt
Stafford

NorthEast
Atchison
Brown
Clay
Doniphan
Douglas
Franklin
Geary
Jackson
Jefferson
Lyon
Marshall
Morris
Nemaha
Osage
Pottawatomie
Riley
Shawnee
Wabaunsee
Washington

EastCentral
Leavenworth
Wyandotte
Johnson
Miami

2017 Q1 CENTRAL MESSAGE SWITCH STATISTICS
JOE MANDALA, CHIEF INFORMATION OFFICER KBI

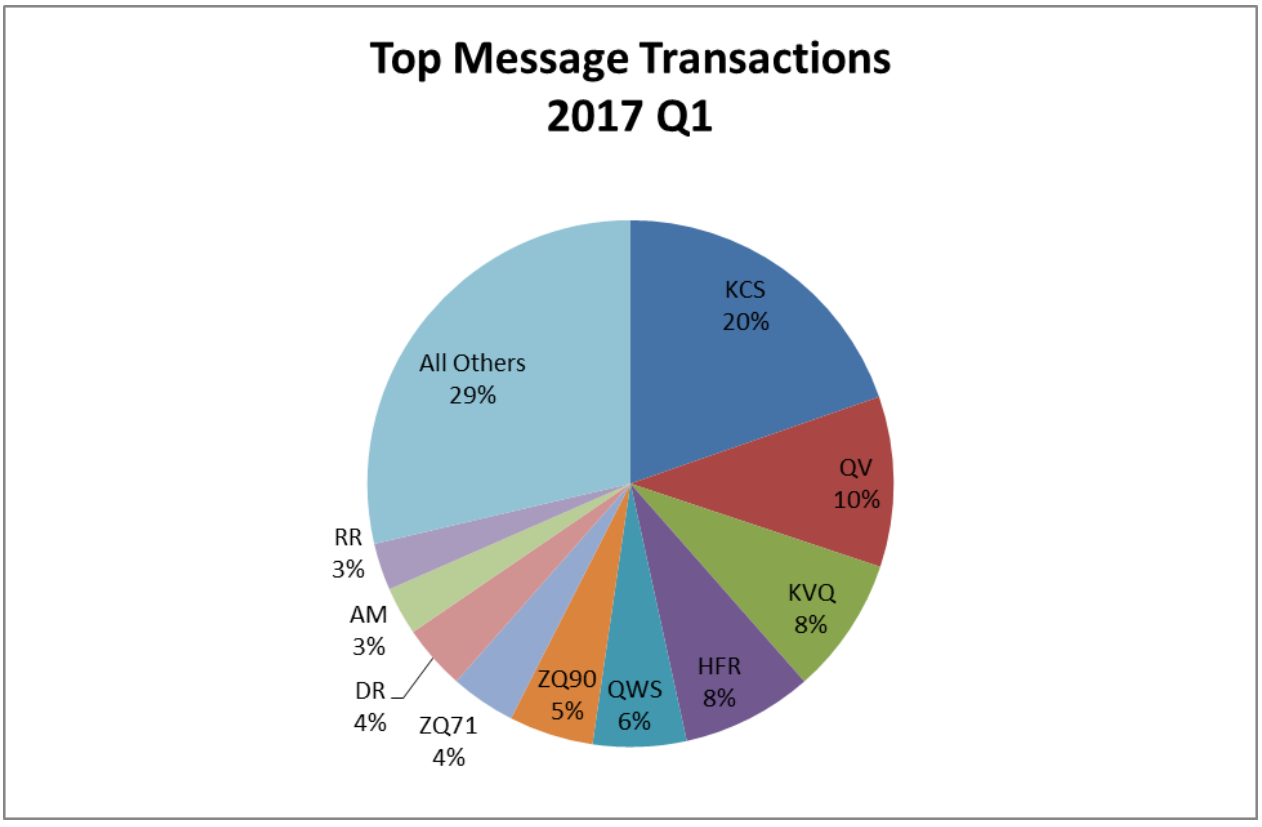
Central Message Switch Statistics, 2017 Q1

The Central Message Switch is a core application in the KCJIS Architecture, and serves a vital function in providing access to a wide variety of information sources critical to the criminal justice system. The Kansas Central Message Switch is accessed by law enforcement agencies, prosecutors, courts, corrections, probation, parole, and other participants in the criminal justice process. It is utilized by local, state, tribal, federal, and international partners.

For the first quarter of 2017, from January through March, the Kansas Central Message Switch processed **27,137,556** transactions. That's an average of nearly **3.5 transactions per second**, 24 hours a day.

Top 10 Message Transactions

These are the most utilized transactions in the Central Message Switch for the reporting period.



MKE	DESCRIPTION	MKE	DESCRIPTION
KCS	KS Car Stop	**ZQ90**	KS Driver Query Name/DOB
QV	NCIC Vehicle Query	**ZQ71**	KS Driver Query OLN
KVQ	KS Vehicle Query	**DR**	NLETS Driver Response
HFR	KS Hotfiles Response	**AM**	NLETS Admin Message
QWS	NCIC Query Wanted State	**RR**	NLETS Registration Response

2017 Q1 CENTRAL MESSAGE SWITCH STATISTICS, CONTINUED
JOE MANDALA, CHIEF INFORMATION OFFICER KBI

Top 10 Utilizing Agencies

These are the 10 agencies that sent the most transactions through the Central Message Switch for the reporting period.

AGENCY	TRANSACTIONS
KANSAS HWY PATROL GENERAL HEADQUARTERS	743,022
SEDGWICK COUNTY SHERIFF'S OFFICE	545,781
WICHITA POLICE DEPARTMENT	363,221
JOHNSON CO SHERIFF'S OFFICE	354,857
TOPEKA POLICE DEPARTMENT	242,726
KANSAS CITY POLICE DEPARTMENT	215,092
RILEY COUNTY POLICE DEPARTMENT	188,622
OVERLAND PARK POLICE DEPARTMENT	148,453
JUNCTION CITY POLICE DEPARTMENT	131,484
GARDEN CITY POLICE DEPARTMENT	128,066

KSORT IS ALIVE AND WELL/OFFENDER REGISTRATION TRAINING
JOHN GAUNTT, OFFENDER REGISTRATION UNIT MANAGER KBI

Since 2013, the Kansas Offender Registration Tool (KsORT), has been used by the majority of Kansas sheriff's offices and the Kansas Department of Corrections to electronically submit offender registration records to the Kansas Bureau of Investigation (KBI). Currently there are 77 KsORT users across our state.

What does using KsORT mean for our Kansas partners? First, it means that an offender's information is updated on the KBI registry, http://www.kbi.ks.gov/registeredoffender/ as quickly as possible. The public has come to expect accurate and timely information about registered offenders and KsORT helps achieve this. Second, KsORT users can view the current database of all Kansas registered offenders. If an offender moves into a county which uses KsORT, all of the current offender information is a click away, right there in KsORT. KsORT users can update an offender's record within minutes. Third, the KBI's offender registration staff supports KsORT users with service and training. If questions come up, you may call the Offender Registration duty phone at (785) 296-2841, or email KBI Offender Registration at registeredoffender@kbi.state.ks.us.

The KBI believes that every criminal justice employee should have a solid foundation of training that corresponds to his or her duties. This is especially true with registered offenders. We encourage every criminal justice employee who has registration duties to request and attend two free KBI training sessions. The first class is on the Kansas Offender Registration Act (KORA), which provides a thorough review of the current statutes that govern registered offenders. The registered offender statutes have been amended by the legislature several times since the KORA became law in 1993. A clear knowledge of the statutes will fundamentally prepare employees for questions that will come up from offenders, the courts, the prosecutor, and the public. A class on the KORA would be a huge confidence builder for the employees responsible for submitting offender records.

The second class is a KsORT training class. We strongly believe that KsORT training would be beneficial to all registering agencies. If your agency uses Offender Watch or submits offender registration records on paper through the mail or by fax, the registration process of offenders is the same. The statutory requirements are the same, no matter how the information gets to the KBI.

In 2015, KBI partnered with Watch Systems to enhance the electronic submission process of offender records. This collaboration has made significant progress over the past year. Both the KBI and Watch Systems have now agreed to emphasize offender registration training of its users to ensure that agencies are trained for consistency and completeness of information. We acknowledge that the repository of offender records is only as good as the information provided by the registering agencies.

KSORT IS ALIVE AND WELL/OFFENDER REGISTRATION TRAINING, CONTINUED
JOHN GAUNTT, OFFENDER REGISTRATION UNIT MANAGER KBI

The KBI also would also invite all Offender Watch using agencies to consider obtaining *read only access* to KsORT. This is another no cost benefit from the KBI to help agencies provide the best service to their area. With read only access, the agency would have the resources available to KsORT users and be able to view the current database of Kansas registered offenders. Read only users would not be able to edit records. With KsORT, you would see the full history of the offender, including all the registration photographs, the vehicles, additional offense information, online identities, and tattoos, just to name a few of the KsORT advantages.

We sincerely hope that every registering agency will soon utilize electronic submissions for their offender records. The KBI has made a firm commitment to Kansas sheriffs to manage the registry with integrity and professionalism. If you have training requests for either KORA or KsORT, please contact Shannon Domingo at Shannon.Domingo@kbi.state.ks.us or (785) 296-1005.

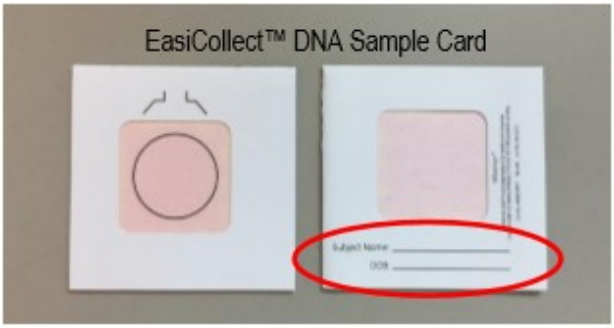
UPDATE FROM THE KBI DNA DATABANK
JESSICA WATTS, LABORATORY TECHNICIAN KBI

During 2016, we had 353 CODIS hits, meaning 353 investigative leads were provided to assist in unsolved cases. As DNA collecting agencies are aware, we have transitioned from using the Bode DNA Collection Kit to using the new GE DNA Collection (EasiCollect™) Kit. If your agency has any stray Bode kits in stock, please discontinue use and discard. If you are unaware how the new collectors look, see the photo below on the right.

Bode DNA Collection Device

GE DNA EasiCollect™ Device

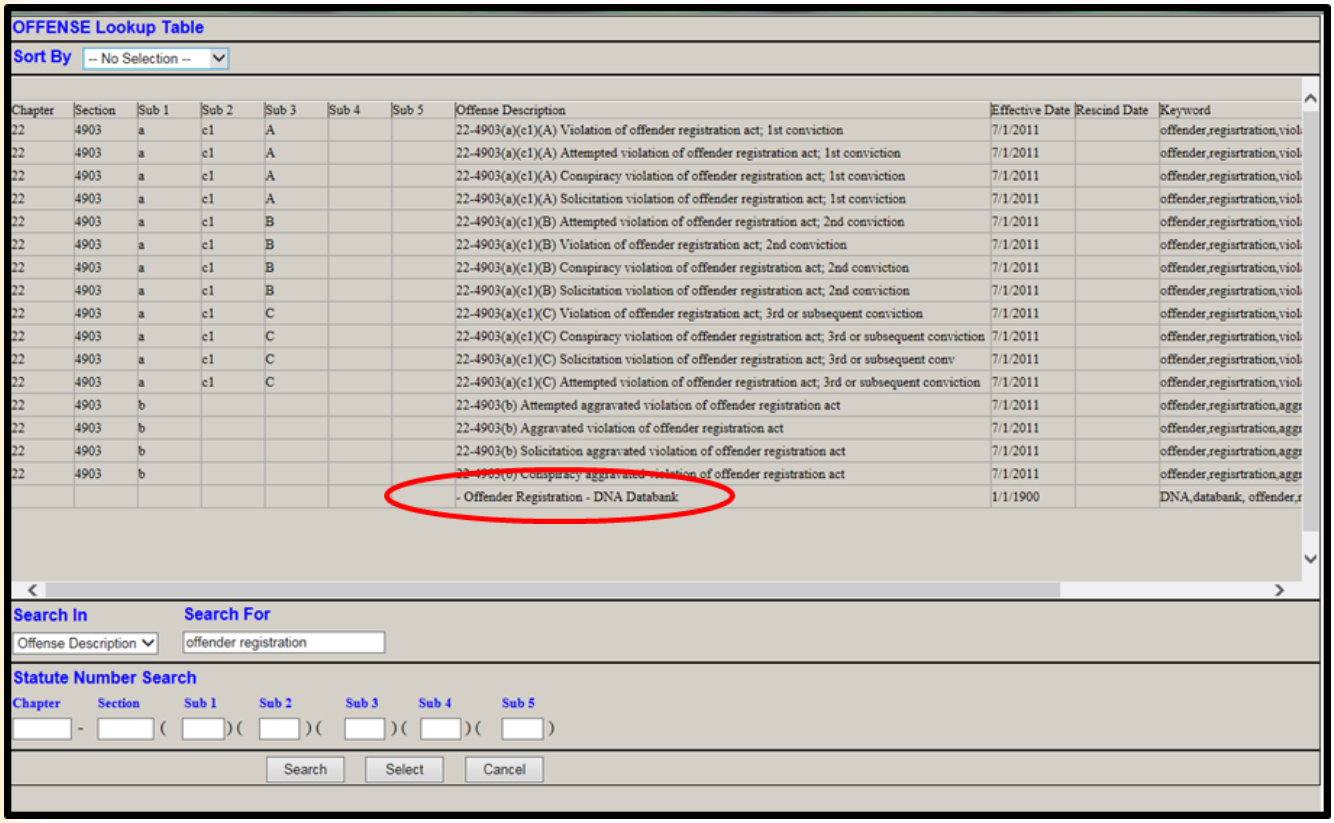
Since the new kits have been deployed we have seen an increase in samples submitted with no name and/or date of birth on the DNA sample card. It has been brought to our attention that collecting agencies did not observe the space provided to write the offender's name and date of birth. The space provided to write the offender's information is on the opposite side of where the sample is collected. Please see the photo below. Writing the offender's information on the DNA sample card is as important as getting the thumbprints collected. The documentation of the offender's information is very important when we have CODIS hits on offenders. Our section utilizes this information to ensure the correct person was collected.



***After the offender is collected, please discard the collection device and submit only the DNA sample card.**

UPDATE FROM THE KBI DNA DATABANK, CONTINUED
JESSICA WATTS, LABORATORY TECHNICIAN KBI

As of July 1, 2016, you may have noticed our state language and some of the subsections have changed. For the collecting agencies using Prelog, you will notice the Computerized Criminal History (CCH) statutes have not been updated yet. We are working on getting this updated. The updated CCH statutes are available for download through the KCJIS network with the use of a token. (Select information>KS State Systems>Statute downloads>CCHstatutesOct2016). Additionally, we have had inquiries about the statute for Offender Registration by collecting agencies using Prelog. There is not a statute number for persons who are required to register as an offender. When entering registered offenders, select 'search type' as the offense description and type in 'offender registration.' Once the search has been deployed, it will present a table with a list as seen in the photo below. Then select 'Offender Registration-DNA Databank.'



Lastly, we have been receiving mailed-in samples with the old laboratory address. Please discontinue and discard any postage-paid envelopes with the old address. A postage-paid envelope with the new laboratory address is included in the EasiCollect™ kits. If any agency received EasiCollect™ kits in the past with the old address, we can send new postage-paid return envelopes to replace them. All kit order requests or questions related to DNA collection should be directed to the DNA Databank contacts or submitted to the address listed below. We appreciate your hard work and attentiveness to offender DNA collection.

DNA Databank Contacts:

Jessica Watts	PH: 785-296-2135	Email: Jessica.Watts@kbi.state.ks.us
Mary Beth Acree	PH: 785-296-2130	Email: MaryBeth.Acree@kbi.state.ks.us

New Laboratory Address:

DNA Databank
KBI Forensic Science Center
2001 SW Washburn Avenue
Topeka, KS 66604

SECURITY AWARENESS REFRESHER
KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT

KCJIS Security Policy 5.2 addresses 'Security Awareness and other Training.' It states that: "basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to Criminal Justice Information (CJI) to include all personnel who have unescorted access to a physically secure location."

Policy subsection 5.2.1 identifies four levels of security awareness training. Level One (5.2.1.1) specifies the topics, which must be addressed as baseline security awareness training for ALL personnel who have unescorted access to a physically-secure location. This would include custodians, maintenance personnel, or any other person who has unescorted access to the physically-secure location. These topics include:

- Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals
- Implications of noncompliance
- Incident response (Identify points of contact and individual actions)
- Visitor control and physical access to spaces - discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

The additional topics in Level Two (5.2.1.2) must be included for all authorized personnel with access to CJI in any form including those that only receive it in hardcopy form.

- Media protection
- Protect information subject to confidentiality concerns—hardcopy (printed material) through destruction
- Proper handling and marking of CJI
- Threats, vulnerabilities, and risks associated with handling of CJI
- Social engineering
- Dissemination and destruction

Level Three (5.2.1.3), builds on that foundation and requires additional topics for all authorized personnel with both physical and logical access to CJI. Physical access is hardcopy. Logical access is computer device access that includes any personnel who use computers that are on the same network others use to access or process CJI.

- Rules that describe responsibilities and expected behavior with regard to information system usage
- Password usage and management - including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code
- Unknown e-mail/attachments
- Web usage - allowed versus prohibited; monitoring of user activity
- Spam
- Physical Security - increases in risks to systems and data
- Handheld device security issues - address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet - address agency policy, procedures, and technical contact for assistance
- Laptop security - address both physical and information security issues
- Personally owned equipment and software - state whether allowed or not (e.g., copyrights)
- Access control issues - address least privilege and separation of duties
- Individual accountability - explain what this means in the agency
- Use of acknowledgement statements - passwords, access to systems and data, personal use and gain
- Desktop security - discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems
- Protect information subject to confidentiality concerns - in systems, archived, on backup media, and until destroyed
- Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services

Level Four (5.2.1.4) has the most topics that must addressed as baseline security awareness training and is for all Information Technology personnel, i.e., system administrators, security administrators, network administrators, etc. These topics look like some repeat, however, this level needs to approach those topics from the administrator perspective rather than a user.

- Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions
- Data backup and storage — centralized or decentralized approach
- Timely application of system patches — part of configuration management
- Access control measures
- Network infrastructure protection measures

SECURITY AWARENESS REFRESHER, CONTINUED
KIP BALLINGER, IT SECURITY AUDITOR/TRAINER KHP CJIS UNIT

Security awareness training would be prudent even if it were not mandatory. Security risks do not go away in the absence of a policy requirement. To reduce your agency's chances of becoming a victim of today's data security threats, you must train everyone; from those who simply have unescorted access to a physically-secure location to those who configure and maintain the information systems.

Insider threats are often more costly or damaging than those committed by external threats. Many agencies do not treat these malicious threats seriously nor do they have adequate safeguards (policies, procedures, practice, tools, etc.) to detect or prevent attacks involving insiders. Insider threats typically do not result from malicious intent, but rather, through negligence or misuse. Outside adversaries do not need to expend the effort to attempt to breach the security controls protecting the boundary of the network if they can obtain the assistance from someone within the agency - preferably someone with administrative or elevated privileges. Enticing an employee to click on a link or pop-up window or to open a common file attachment, such as a PDF or JPG will allow the adversary to install a backdoor tunnel into the information system or to install malicious software, such as keyloggers and screen capture programs.

Therefore, agency personnel should have a good understanding of information security policies and procedures; know how to construct strong, robust passwords; and know how to handle an email from an unknown contact that has an attachment, etc. In order to effect a permanent behavior change, these security and awareness topics need to be reinforced periodically. This is one of the reasons why security awareness training is required biennially. Keep in mind that as a best practice, this training can be done more frequently. The goal is to develop good security habits by knowledge of what to do, skills of how it is done, and positive attitudes. Everyone should understand how to practice good security habits, identifying potential issues, and know how to respond to security incidents.

Security Awareness training material can be found on the KHP Launchpad. Agencies can either administer the training and testing themselves or set their personnel up to take the Security Awareness training through NexTest. Training documents can be found here: https://cjisaudit.khp.ks.gov/launchpad/training/training.cgi?cat_id=4&auth=1&uid= NexTest: https://cjisaudit.khp.ks.gov/nextest/index.cgi

A simple internet search will yield a number of websites, which also provide training information and training for security awareness. These can be good sources as well, provided that they address the baseline security awareness topics required in Policy section 5.2.1.

The KCJIS Newsletter is published in cooperation of the Kansas Criminal Justice Coordinating Council and KCJIS Committee

KCJCC Committee Members

Derek Schmidt
Attorney General
Chair

Sam Brownback
Governor
Vice-Chair

Kirk Thompson
Director
Kansas Bureau of Investigation

Justice Caleb Stegall
Chief Justice Designee

Joe Norwood
Secretary
Kansas Department of Corrections

Mark Bruce
Superintendent
Kansas Highway Patrol

KANSAS BUREAU OF INVESTIGATION

Jessica Crowder
Newsletter Editor
1620 SW Tyler
Topeka, KS 66612
(785) 296-8338
Jessica.Crowder@kbi.state.ks.us

KCJIS Committee Members

Leslie Moore
Kansas Bureau of Investigation
Chair

Sec. Sarah Shipman
KS Department of Administration
Co-Chair

Capt. Lance Royer
KS Sheriffs Association
Treasurer

Ed Klumpp
KS Association of Chiefs of Police
Immediate Past Chair

Steven Zeller
Kansas Highway Patrol

Harold Sass
KS Department of Corrections

Kelly O'Brien
Office of Judicial Administration

Pam Moses
KS Association of District Courts

Amber Norris
KS County and District Attorney Association

Bill Duggan
Lyon CO ECC
KS Assoc. of Public Communications Officers